AFFIDAVIT

STATE OF WASHINGTON ss

COUNTY OF PIERCE

I, KYLE MCNEAL, being first duly sworn on oath, depose and say:

I. INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), assigned to the Special Agent in Charge in Seattle, Washington. I have been an Agent with the FBI since April 2011. As part of my daily duties as an FBI agent, I investigate criminal violations relating to child exploitation and child pornography including violations of Title 18, United States Code §§ 2251(a), 2252A, 2422, and 2423. I have received training in the area of child pornography and child exploitation, and have observed and reviewed numerous examples of child pornography in numerous forms of media, including media stored on digital media storage devices such as computers, iPhones, etc. I have also participated in the execution of numerous search warrants involving investigations of child exploitation and/or child pornography offenses.

2. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant, for the reasons set forth below, to search the following items more fully described in Attachment A for the things specified in Attachment B:

a. SUBJECT DEVICE 1: Samsung Galaxy 9 Cell Phone seized from JONATHAN CARPENTER when he was apprehended on September 17, 2018, and currently in the custody of the FBI;

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3806

b. SUBJECT DEVICE 2: Black iPhone 4, Serial Number C8PHM82FDTF9, received from CHRISTINA CARPENTER on September 17, 2018, and currently in the custody of the FBI;

c. SUBJECT DEVICE 3: Black iPhone 7, Serial Number F17VV8AJHG6W, received from CHRISTINA CARPENTER on September 17, 2018, and currently in the custody of the FBI;

d. SUBJECT DEVICE 4: Red HP Laptop, Serial Number CND61027F3, received from CHRISTINA CARPENTER on September 17, 2018, and currently in the custody of the FBI; and

e. SUBJECT DEVICE 5: Black and Blue Nextbook Laptop, Serial Number YFGV1115014733, received from CHRISTINA CARPENTER on September 17, 2018, and currently in the custody of the FBI.

3. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

4. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are relevant to the determination of probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt/Distribution of Child Pornography), 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), and 18 U.S.C. § 2422(b) (Enticement of a Minor), will be found on the SUBJECT DEVICES.

//

//

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3806

II. SUMMARY OF INVESTIGATION

5. Minor Victim 1 is a 12-year-old boy born in 2006. Minor Victim 2 is an 11-year-old boy born in 2007. On September 17, 2018, MV1 and MV2's mother, Christina Carpenter, notified U.S. Army CID special agents of her concerns that JONATHAN DAVID CARPENTER had sexually abused her son. Christina Carpenter also told agents that MV2 suffers from autism.

6. Interview of Christina Carpenter. The following information was provided from the reports of U.S. Army CID Special Agent Dan Chandler. I have reviewed SA Chandler's reports and described the interviews below. I have not personally reviewed the audio/video recordings of the interviews described. On September 17, 2018, CID agents interviewed Christina Carpenter. She disclosed that on September 11, 2018, MV1 told her that CARPENTER requested the password to MV1's Instagram account and that CARPENTER utilized MV1's Instagram account on MV1's iPhone 7 to request nude images from a female friend of MV1. Christina Carpenter stated that MV1 used a separate phone connected to WiFi to talk to the same female friend while CARPENTER messaged her. MV1 disclosed to Christina Carpenter that MV1 did not feel safe around CARPENTER.

7. Christina Carpenter stated that MV1 disclosed to her in 2015 that CARPENTER digitally penetrated MV1's anus with CARPENTER's finger. Christina Carpenter stated that this disclosure occurred while at their on-post residence located at 5341 Montgomery Street, Joint Base Lewis McChord (JBLM), Washington 98433. This residence is located on the federally owned government property of the JBLM military installation.

8. Christina Carpenter stated that MV2 had also recently disclosed to her that CARPENTER "made him suck his 'pee-pee' until pee came out." Christina Carpenter stated that she did not ask any follow-up questions but told CARPENTER she wanted to seek counseling for the children without CARPENTER present.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3806

9. Interview of MV1. The following information was provided from the reports of U.S. Army CID Special Agent Dan Chandler. I have reviewed SA Chandler's reports and described the interviews below. I have not personally reviewed the audio/video recordings of the interviews described. On September 17, 2018, CID Special Agent (SA) Dan Chandler conducted an interview of MV1. MV1 stated that in 2013 Christina Carpenter left their residence for a period of 11 days. It is believed the family was residing in Watertown, New York, during this time. MV1 stated that during that time, MV1 woke up and needed to go to the bathroom. MV1 stated that he was disoriented and thought the living room was a restroom and began to urinate in the living room. MV1 stated that CARPENTER was naked on the couch while watching the television show "Archer." MV1 stated that CARPENTER scolded him, placed a rag into MV1's mouth and bent MV1 over a chair. MV1 stated that CARPENTER then anally penetrated him with his penis. MV1 stated that when the rag fell out, CARPENTER shoved the rag back into his mouth. MV1 stated that CARPENTER continued to penetrate him for an unknown amount of time. MV1 stated that he went to his room crying and did not know if CARPENTER ejaculated or wore a condom.

10. MV1 stated that a second incident occurred during the same 11-day period when Christina Carpenter was not at the residence. MV1 stated that CARPENTER was laying on the couch naked and called MV1 to him. MV1 stated that CARPENTER then performed oral sex on MV1. CARPENTER then told MV1 "now it's your turn," to which MV1 replied "no," and ran to his room.

11. MV1 stated that a third incident occurred during the same 11-day period when Christina Carpenter was not at the residence. MV1 stated that CARPENTER told him to sleep in CARPENTER's bed, which MV1 did. MV1 woke up later with his clothes removed. MV1 did not know how his clothes removed or anything else that may have transpired while he was sleeping.

12. MV1 stated that sometime in 2015, while living on post at JBLM, he was watching television with MV2. CARPENTER told MV1 to play cards with him. MV1

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3806

stated that CARPENTER told him they would "play like a casino, except instead of chips we use clothes." MV1 disclosed that he and CARPENTER ultimately disrobed while playing CARPENTER's game. MV1 stated that CARPENTER told MV1 to go to CARPENTER's room and lay down. MV1 stated that he went into the room and laid face down. MV1 stated that CARPENTER came into the room and penetrated MV1's anus. MV1 stated that he believed CARPENTER used his finger, but MV1 did not see it. MV1 stated that CARPENTER then rolled onto his back and told MV1 to "suck his dick," to which MV1 said no and ran out of the room. MV1 stated that he disclosed some of the details to Christina Carpenter when she returned home that evening.

13. MV1 stated that in 2015, CARPENTER took MV2 into CARPENTER's room to discipline MV2. MV1 stated that he heard MV2 crying, but did not see what happened in the room. MV1 stated that he discussed with MV2, and that MV2 disclosed that CARPENTER "spanked him" with "his pee-pee."

14. MV1 stated that approximately one week prior to his interview with SA Chandler, MV2 disclosed that CARPENTER forced MV2 to "suck his pee-pee" "until pee came out."

15. MV1 stated that approximately one week prior to his interview with SA Chandler, MV1 provided his iPhone 7 to Carpenter at approximately 10:00 PM, which was standard practice in their home. MV1 stated that he also had an iPhone 4 in his bedroom that CARPENTER was unaware of. MV1 communicated via Instagram direct messages with his female friend "Yasmine" using the iPhone 4. MV1 indicated that Yasmine was a friend who lived out of state, but who attended 4th grade with MV1. MV1 stated that during his conversation with Yasmine, he heard vibrations presumably emanating from a phone. Sometime later, CARPENTER called MV1's name. MV1 stated that CARPENTER came to MV1's bedside and demanded the password for the iPhone 7. MV1 gave CARPENTER the password. MV1 stated that Yasmine related she received an iMessage from MV1's phone number, which read "send nudes." MV1 stated that Yasmine sent him a screenshot which depicted that message. MV1 stated that he did

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3806

not send that message, and it was sent while his iPhone 7 was in the possession of CARPENTER.

16. On September 17, 2018, SA Chandler discussed the details regarding CARPENTER's communication with Christina Carpenter and obtained consent to search for the phones described by MV1. Christina Carpenter provided consent to search and removed both described phones from her purse. SA Chandler documented the identifying information from both phones and collected them for evidentiary purposes. The following phones were collected by SA Chandler:

a. SUBJECT DEVICE 2: Black iPhone 4, Serial Number C8PHM82FDTF9; and

b. SUBJECT DEVICE 3: Black iPhone 7, Serial Number F17VV8AJHG6W

17. Forensic Interview of MV2. The following information was provided from the reports of U.S. Army CID Special Agent Dan Chandler. I have reviewed SA Chandler's reports and described the interviews below. I have not personally reviewed the audio/video recordings of the interviews described. On September 17, 2018, MV2 was interviewed by Susan Villa, Child Forensic Interviewer, Monarch Children's Justice Center in Lacey, Washington. During the forensic interview, MV2 presented apparent difficulty with expressing chronological explanations of all incidents, including descriptions of events not related to the reported offenses. MV2 spoke in disjointed sentences throughout and required multiple questions to clarify details about incidents, including locations of incidents, when incidents occurred, and differentiating two incidents of described oral penetration and two incidents of "humping." Specifically, MV2 required multiple questions to differentiate two incidents of "humping," one in which CARPENTER was wearing shorts and one in which CARPENTER was naked.

18. During the child forensic interview, MV2 provided the following details of his interaction with CARPENTER in CARPENTER's bedroom of the JBLM Montgomery Street duplex in which the family lived. MV2 stated that the following

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3806

incidents occurred while at "the duplex," which Christina Carpenter identified as 5341 Montgomery Street, Joint Base Lewis McChord, Washington. MV2 estimated that the incident occurred about three years prior to the interview with SA Chandler, when MV2 was in 3rd grade. MV2 stated that CARPENTER told MV2 he would get a spanking as discipline for an incident at school. MV2 stated that CARPENTER sent MV2 to CARPENTER's room. MV2 stated that while in CARPENTER's room, CARPENTER told MV2 to "suck [CARPENTER's] 'pee-pee,'" to which MV2 replied "no, am I gay? Are you gay?" MV2 stated that CARPENTER said "just do it," to which MV2 asked "what happens if I don't?" MV2 stated that CARPENTER replied "I'll spank you." MV2 stated that he was sitting on the bed and CARPENTER was standing near the bed. MV2 stated that CARPENTER pulled down CARPENTER's pants. MV2 related that he "sucked [Mr. Carpenter's] 'pee-pee'" and that "pee came out in my mouth." MV2 stated that he "spit that out" in the bathroom, but on another occasion, CARPENTER wanted MV2 to "swallow that."

19. MV2 stated that yet another occasion, CARPENTER bent him over and "put [CARPENTER's] penis in [MV2's] butt" while spanking MV2. MV2 stated CARPENTER went back and forth and was spanking him when he went in and out. MV2 stated that incident occurred when he was in CARPENTER's bedroom.

20. Arrest of CARPENTER. On September 17, 2018, FBI Agents and Lacey Police Department Officers contacted CARPENTER at his residence of 5710 20th Ave SE, Lacey, Washington and placed him under arrest. CARPENTER was then transported to Pierce County Jail. CARPENTER had the following digital device in his possession when he was taken into custody: SUBJECT DEVICE 1: Samsung Galaxy 9 Cell Phone.

21. The following information was taken from FBI Special Agent Richard Schroff's report regarding the collection of digital devices from the residence of 5710 20th Ave SE, Lacey, Washington. While being arrested, CARPENTER advised agents that a 2-year-old child was located inside of the residence. Agents entered the residence to ensure the safety of the child and located the child on the second floor. Agents

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3806

remained with the child at the residence until Christina Carpenter arrived to take custody of the child. After Christina Carpenter was reunited with the child, agents asked for her consent to conduct a search of the residence for electronic devices that CARPENTER may have used. Christina Carpenter provided consent for agents to search the residence. Christina Carpenter described CARPENTER primarily using his cell phone to access the Internet. Christina Carpenter indicated CARPENTER had also used a red laptop (SUBJECT DEVICE 4) and a Nextbook laptop (SUBJECT DEVICE 5) located in the home. Christina Carpenter advised agents that the Nextbook laptop (SUBJECT DEVICE 5) had been "wiped," so it could be provided to one of their children. No areas of the home were searched that were exclusively within the control of CARPENTER, such as his bedside table or dresser.

22. With the consent of Christina Carpenter, the following items were collected from the residence:

a. SUBJECT DEVICE 4: Red HP Laptop, Serial Number CND61027F3; and

b. SUBJECT DEVICE 5: Black and Blue Nextbook Laptop, Serial Number YFGV1115014733.

23. As described above, several of the alleged incidents occurred at an on-post JBLM residence that is located within the special maritime and territorial jurisdiction of the United States and the Western District of Washington.

24. On September 26, 2018, a federal grand jury presiding in the Western District of Washington returned an Indictment against CARPENTER for committing aggravated sexual abuse of a child against MV1 and MV2 in violation of 18 U.S.C. § 2241(c), 2246 and 7.

25. Based on my training and experience as a Special Agent and the information contained in this Affidavit, I submit there is probable cause to believe that JONATHAN DAVID CARPENTER, while living on the JBLM military installation under federal jurisdiction, engaged Attempted Receipt of Child Pornography, Attempted

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3806

Possession of Child Pornography, and Enticement of a Minor, violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), and 18 U.S.C. § 2422(b) (Enticement of a Minor).

III. DEFINITIONS AND TECHNICAL TERMS

26. Set forth below are some definitions of technical terms, most of which are used throughout this Affidavit pertaining to the Internet and computers generally:

a. Computers and digital devices: As used in this Affidavit, the terms "computer" and "digital device," along with the terms "electronic storage media," "digital storage media," and "data storage device," refer to those items capable of storing, creating, transmitting, displaying, or encoding electronic or digital data, including computers, hard drives, thumb drives, flash drives, memory cards, media cards, smart cards, PC cards, digital cameras and digital camera memory cards, electronic notebooks and tablets, smart phones and personal digital assistants, printers, scanners, and other similar items.

b. Internet Service Providers (ISPs) and the storage of ISP records: Internet Service Providers are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e mail, remote storage, and co-location of computers and other communications equipment. ISPs maintain records ("ISP records") pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use.

c. Internet Protocol (IP) Address: Typically, computers or devices on the Internet are referenced by a unique Internet Protocol address the same way every

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3806

telephone has a unique telephone number. An IP address consists of four numeric sequences, separated by a period, and each numeric sequence is a whole number between 0 and 254. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing, that is, they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. The ISP logs the date, time, and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records. Typically, users who sporadically access the Internet via a dial up modem will be assigned an IP address from a pool of IP addresses for the duration of each dial up session. Once the session ends, the IP address is available for the next dial up customer. On the other hand, some ISPs, including some cable providers, employ static IP addressing, that is, a customer or subscriber's computer is assigned one IP address that is used to identify each and every Internet session initiated through that computer. In other words, a static IP address is an IP address that does not change over a period of time and is typically assigned to a specific computer.

d. Hash Value: "Hashing" refers to the process of using a mathematical function, often called an algorithm, to generate a numerical identifier for data. This numerical identifier is called a "hash value" and can be thought of as a "digital fingerprint" for data. If the data that has been "hashed" is changed, even very slightly (like through the addition or deletion of a comma or a period in a text file), the hash value for that data would change. Therefore, if a file such as a digital photo is a hash value match to a known file, it means that the digital photo is an exact copy of the known file.

//

//

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3806

IV. TECHNICAL BACKGROUND

27. As part of my training, I have become familiar with the Internet, a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions, including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via email.

28. Based on my training and experience and information provided to me by computer forensic agents, I know that data can quickly and easily be transferred from one digital device to another digital device. Data can be transferred from computers or other digital devices to internal and/or external hard drives, tablets, mobile phones, and other mobile devices via a USB cable or other wired connection. Data can also be transferred between computers and digital devices by copying data to small, portable data storage devices including USB (often referred to as "thumb") drives, memory cards (Compact Flash, SD, microSD, etc.) and memory card readers, and optical discs (CDs/DVDs).

29. Based on my training and experience, I have learned that the computer's ability to store images and videos in digital form makes the computer itself an ideal repository for child pornography. The size of hard drives used in computers (and other digital devices) has grown tremendously within the last several years. Hard drives with the capacity of four (4) terabytes (TB) are not uncommon. These drives can store thousands of images and videos at very high resolution.

30. Based on my training and experience, collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by companies such as Google, Yahoo, Apple, and Dropbox, among

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3806

others. The online services allow a user to set up an account with a remote computing service that provides email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

31. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" and history files of the browser application used. A forensic examiner often can recover evidence suggesting whether a computer contains wireless software, and when certain files under investigation were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

32. As part of my training and experience, I have become familiar with the structure of the Internet, and I know that connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via email.

33. Based on my training and experience, I know that cellular mobile phones (often referred to as "smart phones") have the capability to access the Internet and store information, such as images and videos. As a result, an individual using a smart phone

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3806

can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smart phone can also easily connect the device to a computer or other digital device, via a USB or similar cable, and transfer data files from one digital device to another. Moreover, many media storage devices, including smartphones and thumb drives, can easily be concealed and carried on an individual's person and smartphones and/or mobile phones are also often carried on an individual's person.

34. As set forth herein and in Attachment B to this Affidavit, I seek permission to search for and seize evidence, fruits, and instrumentalities of the above-referenced crimes that might be found on the SUBJECT DEVICES in whatever form they are found. It has been my experience that individuals involved in child pornography often prefer to store images of child pornography in electronic form. The ability to store images of child pornography in electronic form makes digital devices, examples of which are enumerated in Attachment B to this Affidavit, an ideal repository for child pornography because the images can be easily sent or received over the Internet. As a result, one form in which these items may be found is as electronic evidence stored on a digital device.

35. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals who have a sexualized interest in children and depictions of children:

a. They may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. They may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3806

materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts. These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

c. They often maintain any "hard copies" of child pornographic material that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain these "hard copies" of child pornographic material for many years, as they are highly valued.

d. Likewise, they often maintain their child pornography collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, often at the individual's residence or some otherwise easily accessible location, to enable the owner to view the collection, which is valued highly.

e. They also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. They generally prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

36. In addition to offenders who collect and store child pornography, law enforcement has encountered offenders who obtain child pornography from the internet, view the contents and subsequently delete the contraband, often after engaging in self-gratification. In light of technological advancements, increasing Internet speeds and

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3806

worldwide availability of child sexual exploitative material, this phenomenon offers the offender a sense of decreasing risk of being identified and/or apprehended with quantities of contraband. This type of consumer is commonly referred to as a 'seek and delete' offender, knowing that the same or different contraband satisfying their interests remain easily discoverable and accessible online for future viewing and self-gratification. I know that, regardless of whether a person discards or collects child pornography he/she accesses for purposes of viewing and sexual gratification, evidence of such activity is likely to be found on computers and related digital devices, including storage media, used by the person. This evidence may include the files themselves, logs of account access events, contact lists of others engaged in trafficking of child pornography, backup files, and other electronic artifacts that may be forensically recoverable.

37. Based on my training and experience, and that of computer forensic agents that I work and collaborate with on a daily basis, I know that every type and kind of information, data, record, sound or image can exist and be present as electronically stored information on any of a variety of computers, computer systems, digital devices, and other electronic storage media. I also know that electronic evidence can be moved easily from one digital device to another. As a result, I believe that electronic evidence may be stored on any of the SUBJECT DEVICES.

38. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I believe there is probable cause to believe that the items set forth in Attachment B may be stored on the SUBJECT DEVICES for a number of reasons, including but not limited to the following:

a. Once created, electronically stored information (ESI) can be stored for years in very little space and at little or no cost. A great deal of ESI is created, and stored, moreover, even without a conscious act on the part of the device operator. For example, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache," without the knowledge of the device user. The browser often maintains a fixed amount of hard drive space devoted to

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3806

these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may include relevant and significant evidence regarding criminal activities, but also, and just as importantly, may include evidence of the identity of the device user, and when and how the device was used. Most often, some affirmative action is necessary to delete ESI. And even when such action has been deliberately taken, ESI can often be recovered, months or even years later, using forensic tools.

b. Wholly apart from data created directly (or indirectly) by user-generated files, digital devices - in particular, a computer's internal hard drive - contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible for a user to use such specialized software to delete this type of information - and, the use of such special software may itself result in ESI that is relevant to the criminal investigation. In particular, to properly retrieve and analyze electronically stored (computer) data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the computers. To effect such accuracy and completeness, it may also be necessary to analyze not only data storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the computer and software.

V. SEARCH OF DIGITAL DEVICES

39. In this particular case, and in order to protect the third party privacy of innocent individuals that may have also used the SUBJECT DEVICES, the following are search techniques that will be applied:

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3806

i. Device use and ownership will be determined through interviews, if possible, and through the identification of user account(s), associated account names, and logons associated with the device. Determination of whether a password is used to lock a user's profile on the device(s) will assist in knowing who had access to the device or whether the password prevented access.

ii. Use of hash value library searches.

iii. Use of keyword searches, i.e., utilizing key words that are known to be associated with the sharing of child pornography.

iv. Identification of non-default programs that are commonly known to be used for the exchange and viewing of child pornography, such as, eMule, uTorrent, BitTorrent, Ares, Shareaza, Gnutella, etc.

v. Looking for file names indicative of child pornography, such as, PTHC, PTSC, Lolita, 3yo, etc. and file names identified during the undercover download of child pornography.

vi. Viewing of image files and video files.

vii. As indicated above, the search will be limited to evidence of child pornography and attempts to receive and/or possess child pornography or child erotica but will not include looking for personal documents and files that are unrelated to the crime.

40. These search techniques may not all be required or used in a particular order for the identification of digital devices containing items set forth in Attachment B to this Affidavit. However, these search techniques will be used systematically in an effort to protect the privacy of third parties. Use of these tools will allow for the quick identification of items authorized to be seized pursuant to Attachment B to this Affidavit, and will also assist in the early exclusion of digital devices and/or files which do not fall within the scope of items authorized to be seized pursuant to Attachment B to this Affidavit.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3806

41. In accordance with the information in this Affidavit, law enforcement personnel will execute the search of digital devices seized pursuant to this warrant as follows:

a. The digital devices will be transported to an appropriate law enforcement laboratory for review and to be forensically copied ("imaged").

c. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will produce a complete forensic image, if possible and appropriate, of the SUBJECT DEVICES. In addition, appropriately trained personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data fall within the list of items to be seized pursuant to the warrant. In order to search fully for the items identified in the warrant, law enforcement personnel, which may include investigative agents, may then examine all of the data contained in the forensic image/s and/or on the digital devices to view their precise contents and determine whether the data fall within the list of items to be seized pursuant to the warrant.

d. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this Affidavit.

e. If, after conducting its examination, law enforcement personnel determine that any digital device is an instrumentality of the criminal offenses referenced above, the government may retain that the SUBJECT DEVICE during the pendency of the case as necessary to, among other things, preserve the instrumentality evidence for trial, ensure the chain of custody, and litigate the issue of forfeiture. If law enforcement personnel determine that a device was not an instrumentality of the criminal offenses referenced above, it shall be returned to the person/entity from whom it was seized within 60 days of the issuance of the warrant, unless the government seeks and obtains authorization from the court for its retention.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3806

VI. INSTRUMENTALITIES

42. Based on the information in this Affidavit, I also believe that the SUBJECT DEVICES are instrumentalities of crime and constitute the means by which violations and attempted violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), and 18 U.S.C. § 2422(b) (Enticement of a Minor) have been committed. Therefore, I believe that in addition to seizing the digital devices to conduct a search of their contents as set forth herein, there is probable cause to seize those digital devices as instrumentalities of criminal activity.

VII. CONCLUSION

43. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations and attempted violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), and 18 U.S.C. § 2422(b) (Enticement of a Minor) are located on the SUBJECT DEVICES, as more fully described in Attachment A to this Affidavit. I therefore request that the court issue a warrant authorizing a search of the SUBJECT DEVICES, for the items more fully described in Attachment B hereto, incorporated herein by reference, and the seizure of any such items found therein.

KYLE MCNEAL, Affiant
Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN to before me this 11th day of October, 2018.

J. RICHARD CREATURA
United States Magistrate Judge

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3806